IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

	Kevin Donovan	Examiner:	Dohm Chankong
Application No.:	09/385,802	Group Art Unit:	2152
Filed:	August 30, 1999	Attorney Docket No.:	4031/1 15719US00
For:	Universal Instant Messaging System For The Internet		

DECLARATION of Professor Aviel Rubin Under 37 CFR §1.132

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner Chankong:

I, Aviel Rubin, declare as follows:

1. I hold B.S., M.S., and Ph.D. degrees in Computer Science from the University of Michigan, awarded in 1989, 1991, and 1994 respectively.
2. I am a Professor of Computer Science in the Whiting School of Engineering at The Johns Hopkins University, where I have been a faculty member since 2003. Additionally, I am Technical Director of The Johns Hopkins University Information Security Institute. Prior to 2003, I was an Adjunct Professor at New York University and a Security Researcher at AT&T Labs.
3. I have been retained to give my opinion as to patent application, number 09/385,802, "Universal Instant Messaging System For The Internet," hereto

referred as Donovan. I have read the patent application, cited art, patent claims, the office action dated February 27, 2006, and the claims amendment.

4. U.S. law has often been a restricting factor in the development of cryptographic technologies, which would have discouraged, or lead having one ordinary skill in the art, away from multi-realm instant messaging and encryption.

5. On January 1, 1995, the Communications Assistance for Law Enforcement Act (CALEA) went into effect. This law was designed to aid law enforcement in their clandestine surveillance of citizens via digital networks. The law obligated network service providers to make it possible for law enforcement to undetectably monitor digital network communications. Adding encryption to multi-realm instant messaging would have added so many complications in light of CALEA that messaging service providers would have had good reason to avoid using encryption in their instant messaging services.

6. One of ordinary skill in the art at the time of the Donovan priority date would not have had a reasonable expectation of success in combining the references. In 1991, a version of Netscape's web browser was released that included SSL technology, used for encrypting communication between a client and a server. The SSL-encrypted messages employed the RC4 cipher and 128-bit keys. However, the U.S. government regulations did not permit cryptographic systems that used 128-bit keys to be exported. Netscape was forced to recall their browser, and re-issue an export-compliant edition.

7. Applying encryption to a widely deployed instant messaging system would have been contrary to the accepted wisdom in the art in 1999, and is not mentioned in the cited patents of America Online, Lucent, and Microsoft. Export requirements were relaxed in 2000, but the use of encrypted instant messaging was not widely adopted even half a decade after Donovan's priority date, with the introduction of the Off-the-Record (OTR) Communication plug-in in 2004. Only recently has Apple Computer incorporated encryption into their iChat instant messaging client.
8. The Donovan application is designed to work in different "realms." At about the time of Donovan's priority date, this was a source of much contention. (See "Instant message fight shows power shift," CNET News, July, 1999).
9. In 1999, the exportation of encryption from the United States was approved on a case-by-case basis. Multi-realm encryption with the various messaging service providers cooperating for export approval would not have been expected.
10. Further, as to the level of skill in the art, at the time of the priority date for Donovan, applied cryptography was a specialized and burgeoning field of computer science. Encryption would not have been common skill for an instant messaging programmer to have had in 1999. This is contrary to the examiner's claim that "encryption of network data is rather ubiquitous and even expected in the art."
11. Messaging service providers, like those in the cited art, who make it their business to provide international connectivity, would have been reticent to adopt or

develop any technologies that would narrow the scope of their business. Exporting an encrypting instant messaging service in August 1999 would have been particularly narrowing for a messaging service provider because this would have required users to have computers capable of performing the encryption of instant messages.

12. The art under pinning the rejection does not, in fact, teach what the examiner opines is taught. The Gudjonsson provisional patent application (Gudjon M. Gudjonsson, "A Distributed System to Intelligently Establish Sessions Between Anonymous Users Over Various Networks") does not address the use of encryption to keep communication between two or more parties private; kept secret from both other clients and from the messaging server. In Gudjonsson, encryption is used to securely connect segments of a network, for example, to connect clients to server clusters or to connect server clusters to other server clusters (See pages 4-5 of Gudjonsson). Gudjonsson does not disclose a communication that is encrypted as between two or more clients.
13. In Gudjonsson, a server could read and store messages intended for a client. This is problematic in a multi-realm system that is not necessarily secured or where it may be desirable to hide messages intended only for a client from the servers. Donovan, by contrast, provides encrypted communication as between one more clients. Indeed, the Donovan approach is not a mutually exclusive technology to Gudjonsson, but in fact, may be used as an augmentation to Gudjonsson.

14. The Gudjonsson application relies on cryptography more as an authentication mechanism, rather than an encrypting mechanism as between the users. This is to say, the cryptography used in the Gudjonsson system was primarily used to identify clients to a server, rather than keep their communication private.
15. The Gudjonsson application does not disclose an instant messaging client that would communicate privately with one or more clients through the use of encryption.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon

Respectfully submitted,

Date: 10/11/06

Aviel Rubin

Instant message fight shows power shift

By Jim Hu
Staff Writer, CNET News.com
Published: July 26, 1999, 3:35 PM PDT

In the ongoing fight between America Online, Microsoft, and other players over open standards for instant messaging, it has become increasingly hard to tell who is dominant and who is the underdog.

America Online has entrenched itself in a battle to prevent users of competitors' messaging products from communicating with AOL Instant Messenger (AIM) users. AOL has said it is protecting its users from privacy violations, but critics say it is only protecting its market dominance.

One of those critics, in a curious role-reversal, is Microsoft, which accuses AOL of pretending to stand up for its customers, when it's really only blocking competitors from a market it controls.

For many observers, Microsoft's protests sound odd, given that the company is often criticized for protecting its own market dominance by refusing to open standards. "It's funny hearing Microsoft cry foul over monopolistic practices of a competitor kicking its butt online," said Jupiter Communications analyst Seamus McAteer.

AOL has 40 million registered users on its Buddy List network, which includes AIM and screen names in its proprietary service. Last year it acquired instant messenger ICQ, which has 35 million registered users as of March 1999.

Microsoft's MSN Messenger client, unveiled last week, included a feature that would allow users to communicate with AOL Instant Messenger (AIM) users. Microsoft wants to allow its new MSN Messenger users to access their AIM Buddy Lists.

AOL responded by blocking MSN Messenger--as well as instant messaging clients by Yahoo and Prodigy--from accessing its network. AOL stated it would block all attempts by rival services to access its user base, because the services require users to enter their AOL passwords, which the company deems a privacy violation.

"They are maintaining their hold on what they think is right for their own group of people," a Microsoft spokesman said in a previous interview. AOL is "more focused on maintaining their own situation than what's right for their consumers."

As the rhetoric heats up between the two sides, analysts and observers have noted the power shift that appears to be taking place. AOL in the past has promoted openness in specific areas such as the market for high-speed Net access via cable, citing the need for competition. Meanwhile, Microsoft has embraced openness in this arena despite widespread accusations of monopolistic behavior, including an ongoing antitrust suit being waged by the Justice Department.

Microsoft supports the Internet Engineering Task Force's (IETF) Instant Messaging and Presence Protocol. The group is looking to develop a standard to make competing instant messaging technologies compatible.

For AOL's part, the company says it is in favor of standards, under the right circumstances: "Instant messaging on the Internet will be

open and interconnected, and that's what we should be and that is a goal we certainly support," said AOL spokeswoman Tricia Primrose. "Our view is that without the right coordination, the security and privacy of Internet consumers will be at risk. We have contacted Microsoft to figure out a solution [that is] best for our members and Internet consumers in general."

Some observers say AOL's moves in this area will get it into more trouble down the line with consumer perception and its own efforts to shape the Internet. Instead of rejecting a standard, Rob Enderle, an analyst at Giga Information Group, said AOL should support the standard and become a pacesetter for everyone to follow.

"AOL should embrace the standard effort and take the lead in it," Enderle said. "The aspect of changing a product to block Yahoo and Microsoft is creating an image of a despot, which most likely drives people nuts."

Who's the bully, anyway?

Microsoft itself has long been accused of employing the same tactics for which it now is criticizing AOL. In the early days of the Web, for example, Microsoft tried to keep Netscape Communications away from the browser market, according to a deposition by former Netscape executive Marc Andreessen in the Justice Department's antitrust suit against Microsoft. In exchange, Microsoft offered up access to the closely guarded Windows application programming interfaces (APIs).

Ironically, Netscape is now a division of AOL, and AOL is the one being accused of unfairness by Microsoft.

But Netscape was only one of many software companies that have pointed a finger at Microsoft, saying the company's tight hold on its APIs is tantamount to unfair business practices because of the dominance of the Windows operating system. Oracle, RealNetworks, Sun Microsystems, and others all have argued that Microsoft has an unfair advantage because it has the final say over which APIs make it into Windows.

Last month, for example, Sun Microsystems chief executive Scott McNealy said Microsoft should be forced to open up its application programming interfaces so that software makers are better equipped to use their products with Windows.

But what many in the industry perceive as AOL's defensive stance against open standards has already drawn criticism.

AOL strongly supports the "Open Cable" initiative that calls for cable companies to allow third-party ISPs to sell broadband cable access over their lines. AT&T, which owns cable company Tele-Communications Incorporated and is in the process of acquiring MediaOne, wants to keep cable lines closed. The telecommunications giant also owns cable Internet access provider Excite@Home, which it plans to use as the high-speed ISP for its spate of cable access services.

Today AT&T general counsel Jim Cicconi responded to AOL's moves, calling the company's efforts to keep its instant messaging service closed hypocritical and a reflection of its own "disingenuousness."

"It's ironic that AOL--for the last several months holding itself out as the protector of 'openness' on the Internet--has now made evident the closed nature of its own system by sabotaging instant messaging communications between its customers and those of other ISPs," Ciccone said. "AOL's ongoing effort to leverage its market power to block communication among Internet users who refuse to use AOL's proprietary system is hypocritical and antithetical to the very ethos of the Internet."

But AOL's Primrose maintained that the company's moves were made to protect users' privacy: "When I see a product that risks privacy of consumers, I ask the question, 'Who is serving the consumer best?'"

The Netscape factor

AOL critics also point to its Netscape subsidiary, which is one of the most vocal proponents of open standards on the Web, as a source of conflicting agendas. Netscape established Mozilla.org in January

1998 to shepherd open-source development of its Communicator browser. Netscape began publishing its source code in response to Microsoft's Internet Explorer browser chipping away at its once-dominant market share.

Netscape is also spearheading the Open Directory initiative, which stems from its acquisition of Newhoo earlier this year. The project is charged with creating a directory of Web sites generated from the grassroots level. Lycos recently signed on to use the service.

A leader is still a leader

Still, for Jupiter's McAteer, the demand among competitors for standards simply illustrates further the momentum AOL has behind it in the instant messaging space.

Jupiter's McAteer compared AOL's instant messenger dominance to Microsoft's own dominance in operating systems. Both are killer applications that have accelerated the maturation of their markets in the Internet and desktop PCs, respectively. And both applications are making their markets more used in everyday life.

"There is something to be said for proprietary technologies, especially if you want to drive a platform quickly," McAteer said. "Microsoft has lost this battle...they've all lost this battle."